This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of monitoring a registry comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests, wherein at least one security clearance parameter is updated by a system command in association with one or more of the requests.

2. (original) The method of claim 1 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

3. (original) The method of claim 1 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

4. (original) The method of claim 1 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

5. (currently amended) A registry monitoring system wherein the registry is monitored by a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests, wherein at least one security clearance permission is reestablished in association with one or more of the requests.

6. (original) The registry monitoring system of claim 5 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

7. (original) The registry monitoring system of claim 5 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

8. (original) The registry monitoring system of claim 5 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

9. (currently amended) A computer configured to monitor a registry according to a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; ~~and~~

obtaining security clearance to complete the requests; and

updating at least one security clearance parameter in association with one or more of the requests.

10. (original) The computer of claim 9 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

11. (original) The computer of claim 9 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

12. (original) The computer of claim 9 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

13. (currently amended) A machine-readable medium comprising a program to monitor a registry according to a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; ~~and~~

obtaining security clearance to complete the requests; and

updating at least one security clearance permission.

14. (original) The machine-readable medium of claim 13 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

15. (original) The machine-readable medium of claim 13 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

16. (original) The machine-readable medium of claim 13 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

17. (currently amended) A computer implemented secured data transmission system having a receiver to access secured file content provided by a sender, wherein the receiver includes a registry monitoring system wherein the registry is monitored by a method comprising:

requesting a handle for a registry key to a calling process;

requesting a registry key value for the handle; and

obtaining security clearance to complete the requests, wherein at least one security clearance parameter is updated via a system command in association with one or more of the requests.

18. (original) The computer implemented secured data transmission system of claim 17 further comprising after requesting a handle for a registry key to a calling process:

determining a process ID and registry key;

determining whether the process is secured by checking a secured process list;

if the process is secured, determining whether the registry key is on a rejection list;

if the registry key is on the rejection list, denying the process access to the registry key; and

if the process is not on the secured list or if the registry key name is not on the rejection list, completing the request.

19. (original) The computer implemented secured data transmission system of claim 17 further comprising after requesting a registry key value for the handle:

determining a process ID and registry key value;

determining whether the process is secured by checking the secured process list;

if the process is secured, determining whether the registry key is on the rejection list;

if the registry key is on the rejection list, denying the process access to the registry key value;

if the process is not on the secured list, completing the request;

if the registry key is not on the rejection list and the process is on the secured process list, processing the value request and determining whether the value is on the rejection list;

if the value is not on the rejection list allowing the request to be completed; and

if the value is on the rejection list denying access to the registry key value.

20. (original) The computer implemented secured data transmission system of claim 17 further comprising after modifying and deleting handles and values:

determining a process ID;

determining whether the process is secured by checking whether the process is on the secured process list;

if the process is not on the secured process list, completing the request; and

if the process is on the secured process list, not allowing the request to be completed.

21. (new) A registry monitoring system comprising:

at least one machine-readable medium for:

receiving a handle request for a registry key to a calling process; receiving a registry key value request for the handle; granting security clearance to complete the requests; and updating at least one security clearance permission by a system command.

22. (new) The registry monitoring system of claim 21, further comprising denying security clearance when at least one security clearance permission is satisfied.

23. (new) The registry monitoring system of claim 21, wherein said at least one security clearance permission is associated with the elapsed time since said handle or registry key value has been previously requested.

24. (new) The registry monitoring system of claim 21, wherein said at least one security clearance permission is associated with the number of times said handle or registry key value has been previously requested.

25. (new) The registry monitoring system of claim 21, wherein said at least one security clearance permission is associated with the date in which said handle or registry key value was previously requested.

26. (new) The registry monitoring system of claim 21, wherein said at least one security clearance permission is associated with the accumulated time said handle or registry key value has been previously accessed.

27. (new) The registry monitoring system of claim 26, wherein said previous access includes modifying and deleting keys and values of protected data locations.

28. (new) The registry monitoring system of claim 21, wherein said at least one machine-readable medium includes at least one device driver.

29. (new) A method of monitoring a registry comprising:

receiving a handle request for a registry key to a calling process;

receiving a registry key value request for the handle;

granting security clearance to complete the requests; and

updating at least one security clearance parameter.

30. (new) The method of claim 29, further comprising denying security clearance when at least one security clearance parameter is satisfied.

31. (new) The method of claim 29, wherein said at least one security clearance parameter is associated with the elapsed time since said handle or registry key value has been previously requested.

32. (new) The method of claim 29, wherein said at least one security clearance parameter is associated with the number of times said handle or registry key value has been previously requested.

33. (new) The method of claim 29, wherein said at least one security clearance parameter is associated with the date in which said handle or registry key value was previously requested.

34. (new) The method of claim 29, wherein said at least one security clearance parameter is associated with the accumulated time said handle or registry key value has been previously accessed.

35. (new) The method of claim 34, wherein said previous access includes modifying and deleting keys and values of protected data locations.